Le problème de Waring

Arthur Touati

28 décembre 2018

Résumé

La notion de dénombrabilité ne permet pas de distinguer l'ensemble des entiers impairs de l'ensemble des nombres premiers (ils sont tous les deux en bijection avec $\mathbb{N}$). Notre intuition nous dit pourtant que le premier est "plus gros" que le deuxième... Il nous faut donc une notion permettant de rafiner notre étude des sous-ensembles de $\mathbb{N}$. La densité de Schnirelmann est une solution à ce problème.

Après avoir définit et étudié la densité de Schnirelmann, nous verrons comment elle permet l'accès à des résultats arithmétiques compliqués, en l'appliquant au problème de Waring.

La plupart des preuves sont tirées du livres *Three Pearls Of Number Theory* d'Alexandre Khinchin, publié en 1952.

1 Borne supérieure et inférieure d'une partie de $\mathbb{R}$

Soit A un sous-ensemble de $\mathbb{R}$.

Définition 1.1. *On dit que $m \in \mathbb{R}$ est un minorant de A lorsque :*

$$\forall x \in A, \quad m \leq x.$$

On dit que $M \in \mathbb{R}$ est un majorant de A lorsque :

$$\forall x \in A, \quad x \leq M.$$

Exercice 1. Y-a-t-il toujours existence et unicité d'un minorant ?

Définition 1.2. *On dit que A est minorée si elle admet au moins un minorant et qu'elle est majorée si elle admet au moins un majorant.*

Définition 1.3. *Soit $m \in \mathbb{R}$, on dit que m est le minimum de A si $m \in A$ et si m est un minorant de A, on le note* $\min A$.

On définit de même le maximum d'une partie.

Exercice 2. Y-a-t-il toujours existence et unicité du minimum ?

L'ensemble $]0, 1]$ n'admet pas de minimum alors qu'il est bien minorée (par 0). Pourtant on sent bien que 0 joue un rôle particulier parmi les minorants de cet ensemble, cela motive la définition suivante.

Définition 1.4. *Si $\{x \in \mathbb{R} \mid x \text{ minore } A\}$ admet un maximum, on définit la borne inférieure de A comme*

$$\inf A = \max \{x \in \mathbb{R} \mid x \text{ minore } A\}.$$

Il faut retenir que la borne inférieure d'une partie (si elle existe) est le plus grand des minorants, c'est le "meilleur" minorant. On définit de la même manière la borne supérieure d'un ensemble comme le plus petit des majorants. On peut vérifier que 0 est la borne inférieure de $]0,1]$ sans être pour autant son minimum. Le lien entre borne inférieure est minimum d'une partie est le suivant : si $\inf A$ existe et vérifie $\inf A \in A$, alors $\inf A = \min A$.

On peut énoncer la caractérisation suivante, utile pour calculer la valeur d'une borne inférieure (ou supérieure).

Proposition 1.1. *Soit $m \in \mathbb{R}$, on a :*

$$m = \inf A \iff \begin{cases} \forall a \in A, \quad m \leq a \\ \forall \varepsilon > 0, \quad \exists a \in A, \quad a \leq m + \varepsilon \end{cases}.$$

Dans la pratique, nous utiliserons le critère suivant, qui découle de la proposition 1.1 :

Proposition 1.2. *Soit $A \subset \mathbb{R}$, et $m \in \mathbb{R}$, $m = \inf A$ si et seulement si m minore A et s'il existe une suite d'éléments de A convergeant vers m.*

La théorème suivant est une conséquence de l'axiomatique de $\mathbb{R}$, c'est la raison pour laquelle nous ne le démontrons pas.

Théorème 1.1. *Toute partie de $\mathbb{R}$ minorée admet une borne inférieure.*

De la même manière, toute partie majorée admet une borne supérieure. Pour terminer cette partie, voici deux exercices de détermination de bornes supérieures et inférieures.

Exercice 3. On considère $A = \left\{ \frac{1}{p} + \frac{1}{q} \;\middle|\; p, q \in \mathbb{N}^* \right\}$, prouver l'existence et donner les valeurs de $\inf A$ et $\sup A$.

Exercice 4. On considère $A = \left\{ \frac{mn}{(m+n)^2} \;\middle|\; m, n \in \mathbb{N}^* \right\}$, prouver l'existence et donner les valeurs de $\inf A$ et $\sup A$.

2 La densité de Schnirelmann

Nous allons maintenant nous intéresser aux parties de $\mathbb{N}$ et définir la densité de Schnirelmann. Si $A \subset \mathbb{N}$ est une partie finie, on note $|A|$ son cardinal et on définit $A(n)$ par :

$$A(n) = |A \cap \{1, \ldots, n\}|.$$

2.1 Définition et premières propriétés

Définition 2.1. *Soit $A \subset \mathbb{N}$, la densité de Schnirelmann de A est le réel*

$$\sigma(A) = \inf \left\{ \frac{A(n)}{n} \;\middle|\; n \in \mathbb{N}^* \right\}.$$

Pour toute partie $A \subset \mathbb{N}$, l'ensemble $\left\{ \frac{A(n)}{n} \;\middle|\; n \in \mathbb{N}^* \right\}$ est minorée par 0 donc sa borne inférieure existe bien. La densité de Schnirelmann est une mesure de la répartition des éléments de A parmi les entiers naturels, d'où le terme de densité.

Proposition 2.1. *Soit $A \subset \mathbb{N}$, on a les propriétés suivantes :*

1. $0 \leq \sigma(A) \leq 1$.
2. $\forall n \in \mathbb{N}^*, \quad n\sigma(A) \leq A(n)$.
3. $\sigma(A) = 1 \Longrightarrow A = \mathbb{N}^*$.
4. $1 \notin A \Longrightarrow \sigma(A) = 0$.

5. *si $\sigma(A) = 0$ et $1 \in A$, alors pour tout $\varepsilon > 0$, il existe une suite $(n_k)_{k\in\mathbb{N}^*}$ qui tend vers $+\infty$ et telle que $A(n_k) \leq \varepsilon n_k$ et .*

Démonstration. 1. Pour $n \in \mathbb{N}^*$, on a $A \cap \{1, \dots, n\} \subset \{1, \dots, n\}$ donc $A(n) \leq n$ d'où $0 \leq \frac{A(n)}{n} \leq 1$.

2. Par définition, la borne inférieure est un minorant donc pour tout $n \in \mathbb{N}^*$, on a $\sigma(A) \leq \frac{A(n)}{n}$.

3. Si $\sigma(A) = 1$, alors pour tout $n \in \mathbb{N}^*$, on a $A(n) = n$, ce qui implique $A \cap \{1, \dots, n\} = \{1, \dots, n\}$, ce qui implique $A = \mathbb{N}^*$.

4. Si $1 \notin A$, alors $A(1) = 0$ et 0 est donc le minimum de $\left\{ \frac{A(n)}{n} \;\middle|\; n \in \mathbb{N}^* \right\}$, ce qui donne le résultat.

5. C'est une conséquence directe de la caractérisation de la borne inférieure, et du fait que si $1 \in A$, alors $\frac{A(n)}{n} > 0$ pour tout $n \in \mathbb{N}^*$.

□

2.2 Exemples

Nous allons maintenant donner des exmples de calculs explicites de densités de Schnirelmann, qui montrent l'intérêt de cette notion.

Proposition 2.2. *Si $A \subset \mathbb{N}$ est fini, alors $\sigma(A) = 0$.*

Démonstration. Si A est fini, il admet un plus grand élément qu'on note M. Pour tout $n \geq M$, on a $\frac{A(n)}{n} = \frac{M}{n}$ qui converge vers 0. On utilise alors la proposition 1.2. □

Dans la suite, on note $E(x)$ la partie entière d'un réel x, c'est-à-dire l'unique entier vérifiant $x - 1 < E(x) \leq x$. Le fait d'être de densité nulle n'implique pas pour autant que l'ensemble A est fini, comme le montre certains des exmples suivants :

Proposition 2.3. *La densité de $\{2n \mid n \in \mathbb{N}^*\}$ est 0, la densité de $\{2n + 1 \mid n \in \mathbb{N}\}$ est $\frac{1}{2}$.*

Démonstration. L'ensemble des entiers naturels pairs ne contient pas 1 et d'après la proposition 2.1 sa densité est nulle. On note I l'ensemble des entiers naturels impairs, un calcul simple donne $I(n) = E\left(\frac{n+1}{2}\right)$. On pose $u_n = \frac{E\left(\frac{n+1}{2}\right)}{n}$, nous allons montrer que la suite $(u_n)_{n\in\mathbb{N}}$ converge vers $\frac{1}{2}$ et est minorée par $\frac{1}{2}$, ce qui donnera le résultat, par la proposition 1.2. De l'encadrement $x - 1 < E(x) \leq x$, on obtient $\frac{n-1}{2n} < u_n \leq \frac{n+1}{2n}$ ce qui montre que la suite converge vers $\frac{1}{2}$. De plus, $u_{2n+1} = \frac{n+1}{2n} \geq \frac{1}{2}$ et $u_{2n} = \frac{1}{2}$ donc pour tout $n \in \mathbb{N}^*$ on a $u_n \geq \frac{1}{2}$. □

Proposition 2.4. *Pour tout $n \geq 2$, on a $\sigma(A_n) = 0$, où $A_n = \{p^n \mid p \in \mathbb{N}\}$.*

Démonstration. Pour $k, p \in \mathbb{N}^*$, on a $1 \leq p^n \leq k$ si et seulement si $1 \leq p \leq E(k^{\frac{1}{n}})$, on a donc $A_n(k) = E(k^{\frac{1}{n}})$. On pose $u_k = \frac{E(k^{\frac{1}{n}})}{k}$, montrons que la suite $(u_k)_{k\in\mathbb{N}}$ converge vers 0, ce qui donnera le résultat, toujours grâce à la proposition 1.2. De l'encadrement $E(x) \leq x$, on obtient $0 \leq u_k \leq k^{\frac{1}{n}-1}$ ce qui montre que $(u_k)_{k\in\mathbb{N}}$ converge vers 0 (car $n \geq 2 \Longrightarrow \frac{1}{n} - 1 < 0$). □

3 Les bases additives

3.1 Somme d'ensembles

Nous allons nous intéresser au comportement de la densité de Schnirelmann vis-à-vis de l'addition, que se passe-t-il si on ajoute deux ensembles ? et d'abord, comment ajoute-t-on des sous-ensembles de $\mathbb{N}$?

Définition 3.1. *Soit $A, B \subset \mathbb{N}$, on définit leur somme $A \oplus B$ par :*

$$A \oplus B = \{a + b \mid a \in A,\ b \in B\} \cup A \cup B.$$

Une remarque importante est la suivante : si $0 \in A \cap B$, alors $A \oplus B = \{a + b \mid a \in A,\ b \in B\}$. La loi de composition interne $\oplus$ est commutative et associative, on peut donc effectuer la somme de plusieurs ensembles sans se soucier de l'ordre et du parenthésage. Soit $A \subset \mathbb{N}$, on note nA l'ensemble $A \oplus \ldots \oplus A$ où il y a n copies de A dans la somme.

Donnons des exemples de calculs de sommes d'ensembles :

1. Si A et B sont des ensembles finis, alors $A \oplus B$ est aussi fini.
2. On a $\{1\} \oplus \{2n \mid n \in \mathbb{N}\} = \mathbb{N}$, c'est un exemple où $\sigma(A) = \sigma(B) = 0$ et $\sigma(A \oplus B) > 0$.
3. On a $2I = \mathbb{N}^*$.

Une question importante en théorie des nombres est la suivante : si $A \subset \mathbb{N}$ est donné, est-ce que tout entier naturel n peut s'écrire comme somme d'éléments de A ? si oui, est-ce que le nombre de termes dans la somme dépend de n ? Ces questions motivent la définition suivante.

Définition 3.2. *Soit $A \subset \mathbb{N}$, on dit que A est une base additive s'il existe un entier k vérifiant $kA = \mathbb{N}$.*

3.2 Le théorème de Schnirelmann

Dans cette partie nous allons considérer deux parties $A, B \subset \mathbb{N}$, telles que $0 \in A \cap B$ (de telle sorte que $A \oplus B = \{a + b \mid a \in A,\ b \in B\}$) et définir la suite des éléments de A et B rangés dans l'ordre croissant :

$$A = \{0, a_1, \ldots, a_n, \ldots\}$$
$$B = \{0, b_1, \ldots, b_n, \ldots\}$$

On considère uniquement le cas des ensembles infinis. On peut toujours se ramener au cas où $0 \in A \cap B$, car si $C \subset \mathbb{N}$, on a $\sigma(C) = \sigma(C \cup \{0\})$.

Proposition 3.1. *Soit $A, B \subset \mathbb{N}$, on a :*

$$\sigma(A \oplus B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B).$$

Démonstration. Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{N}^*$ tels que $a_k, a_{k+1} \in [\![1, n]\!]$. Comme on a rangé les a_i de manière strictement croissante, on a $[\![a_k + 1, a_{k+1} - 1]\!] \cap A = \emptyset$, cet intervalle contient $\ell = a_{k+1} - a_k - 1$ entiers, ceux de la forme, $a_k + r$ pour $r \in [\![1, \ell]\!]$. Combien de ces entiers appartiennent à $A \oplus B$? Il faut et il suffit que $r \in B$, il y a donc $B(\ell)$ possibilité. Donc à chaque séquence de longueur ℓ entre deux éléments consécutifs de $A \cap [\![1, n]\!]$, il y a $B(\ell)$ entiers appartenant à $A \oplus B$, on a donc la minoration suivante :

$$(A \oplus B)(n) \geq A(n) + \sum_{\ell \in \mathfrak{L}_n} B(\ell),$$

où $\mathfrak{L}_n$ est l'ensemble des entiers ℓ tels qu'il existe une séquence de longueur ℓ entre deux éléments consécutifs de $A \cap [\![1, n]\!]$. On a supposé qu'il existait au moins deux éléments de A dans $[\![1, n]\!]$, si ce n'est pas le cas, on voit que cet inégalité tient toujours, la suite du raisonnement est donc vraie pour tout entier naturel n.

On utilise maintenant le fait que $B(\ell) \geq \ell\sigma(B)$:

$$(A \oplus B)(n) \geq A(n) + \sigma(B) \sum_{\ell \in \mathfrak{L}_n} \ell.$$

Or, en se rappelant de la définition de $\mathfrak{L}_n$, on montre facilement que $\sum_{\ell \in \mathfrak{L}_n} \ell = n - A(n)$, on obtient alors :

$$(A \oplus B)(n) \geq A(n)(1 - \sigma(B)) + n\sigma(B).$$

Comme $1 - \sigma(B) \geq 0$, on a $A(n)(1 - \sigma(B)) \geq n\sigma(A)(1 - \sigma(B))$ et :

$$(A \oplus B)(n) \geq n\sigma(A)(1 - \sigma(B)) + n\sigma(B) \iff \frac{(A \oplus B)(n)}{n} \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B).$$

Cette inégalité étant vraie pour tout $n \in \mathbb{N}^*$, on obtient le résultat voulu. □

En remarquant que $\sigma(A)+\sigma(B)-\sigma(A)\sigma(B) = 1-(1-\sigma(A))(1-\sigma(B))$, on peut étendre cette minoration à plus de deux ensembles :

Proposition 3.2. *Pour toute famille finie $(A_i)_{i \in [1,n]}$ de sous-ensembles de $\mathbb{N}$ contenant 0, on a :*

$$\sigma\left(\bigoplus_{i=1}^{n} A_i\right) \geq 1 - \prod_{i=1}^{n}(1 - \sigma(A_i)).$$

Démonstration. On va raisonner par récurrence sur le cardinal de la famille : si c'est vrai au rang $n \in \mathbb{N}^*$, soit $(A_i)_{i \in [1,n+1]}$ une famille de sous-ensembles de $\mathbb{N}^*$. On a :

$$\begin{aligned}
\sigma\left(\bigoplus_{i=1}^{n+1} A_i\right) &= \sigma\left(A_{n+1} \oplus \bigoplus_{i=1}^{n} A_i\right) \\
&\geq \sigma(A_{n+1}) + \sigma\left(\bigoplus_{i=1}^{n} A_i\right) - \sigma(A_{n+1})\sigma\left(\bigoplus_{i=1}^{n} A_i\right) \\
&= 1 - (1 - \sigma(A_{n+1}))\left(1 - \sigma\left(\bigoplus_{i=1}^{n} A_i\right)\right) \\
&\geq 1 - (1 - \sigma(A_{n+1}))\prod_{i=1}^{n}(1 - \sigma(A_i)) \\
&= 1 - \prod_{i=1}^{n+1}(1 - \sigma(A_i)).
\end{aligned}$$

□

Maintenant que l'on connait le comportement de la densité de Schnirelmann vis-à-vis de la somme d'ensemble, il nous faut un critère efficace pour montrer qu'une somme d'ensembles engendre tout $\mathbb{N}$:

Proposition 3.3. *Si $A, B \subset \mathbb{N}$ contiennent O, alors :*

$$\sigma(A) + \sigma(B) \geq 1 \Longrightarrow A \oplus B = \mathbb{N}.$$

Démonstration. Soit $n \geq 1$, nous allons commencer par montrer que si $A(n) + B(n) \geq n$, alors $n \in A \oplus B$. Si $n \in A \cup B$ c'est effectivement le cas, supposons donc que $n \notin A \cup B$. On a alors $A(n) = A(n-1)$ et $B(n) = B(n-1)$. On considère la famille

$$\{a_1, \ldots, a_{A(n-1)}, n - b_1, \ldots, n - b_{B(n-1)}\}.$$

Ces entiers appartiennent tous à $[\![1, n-1]\!]$ et il y en a $A(n-1) + B(n-1) \geq n$. Par le principe des tiroirs, deux d'entre doivent être égaux. Comme on ne peut pas avoir $a_i = a_j$ ou $b_i = b_j$ pour $i \neq j$, il existe nécessairement $(i, j) \in [\![1, A(n-1)]\!] \times [\![1, B(n-1)]\!]$ tel que $a_i = n - b_j$, ce qui implique que $n \in A \oplus B$.

Pour montrer le résultat, il ne nous reste plus qu'à remarquer que si $\sigma(A) + \sigma(B) \geq 1$, alors $A(n) + B(n) \geq n$ pour tout $n \in \mathbb{N}^*$, ce qui conclut. □

Nous pouvons maintenant énoncer et démontrer le théorème de Schnirelmann, qui donne un critère "simple" pour déterminer si une partie de $\mathbb{N}$ est une base additive.

Théorème 3.1. *Si $A \subset \mathbb{N}$ est tel que $\sigma(A) > 0$, alors A est une base additive.*

Démonstration. On applique la proposition 3.2 dans le cas où $A_i = A$ pour tout i. Pour tout $n \in \mathbb{N}^*$, on a donc

$$1 - \sigma(nA) \leq (1 - \sigma(A))^n.$$

Si $\sigma(A) > 0$, le membre de droite est une suite convergeant vers 0, il existe donc $k \in \mathbb{N}^*$ tel que $(1 - \sigma(A))^k \leq \frac{1}{2}$, on a donc $\sigma(kA) + \sigma(kA) \geq 1$, ce qui d'après la proposition 3.3 implique que $2kA = \mathbb{N}^*$. □

Il est intéressant de remarquer que la proposition 3.1 n'est pas le résultat optimal sur la question. En 1942, Henry Mann montra qu'en réalité on a toujours $\sigma(A \oplus B) \geq \sigma(A) + \sigma(B)$. La preuve de ce résultat est longue et compliquée, nous ne la donnons pas ici (elle se trouve dans le livre de Khinchin) car nous n'utilisons pas ce théorème.

4 Le problème de Waring

En théorie des nombres, le problème de Waring, proposé en 1770 par Edward Waring consiste à déterminer si, pour chaque entier naturel k, il existe un nombre s tel que tout entier positif soit somme de s puissances k-ièmes d'entiers positifs. En 1909, David Hilbert apporta une réponse affirmative au problème. Nous allons exposé la preuve donné en 1942 par Linnik, qui reste à ce jour la plus élémentaire (tout en restant assez difficile...).

Dans toute la suite, $n \geq 2$ est un entier naturel fixé. On note :

$$A_n = \{p^n \mid p \in \mathbb{N}\}.$$

On a vu que $\sigma(A_n) = 0$, la question est de savoir s'il existe un entier $N \geq 2$ tel que $\sigma(NA_n) > 0$. Si c'est le cas, le théorème de Schnirelmann nous dit que NA_n est une base additive, et donc que A_n en est une aussi, ce qui répond affirmativement au problème de Waring. Nous allons démontrer le théorème suivant :

Théorème 4.1. *Il existe un entier N, ne dépendant que de n, tel que $\sigma(NA_n) > 0$.*

4.1 Preuve du théorème

A quelle condition un entier m appartient à kA_n ? C'est le cas si et seulement l'équation suivante admet au moins une solution $(x_1, \dots, x_k) \in \mathbb{N}^k$:

$$x_1^n + \cdots + x_k^n = m. \tag{1}$$

On note $r_k(m)$ le nombre de solutions de l'équation 1 dans $\mathbb{N}^k$, de telle sorte que $m \in kA_n$ si et seulement si $r_k(m) > 0$. Nous allons admettre pour l'instant le lemme fondamental suivant :

Lemme 4.1 (Lemme fondamental)**.** *Il existe $k \in \mathbb{N}$ et $C > 0$ tels que pour tout $N \in \mathbb{N}$:*

$$\forall m \in [\![1, N]\!], \quad r_k(m) < CN^{\frac{k}{n}-1}.$$

Il nous reste deux objectifs : montrer le théorème en admettant le lemme fondamental, et prouver le lemme fondamental. Le deuxième objectif est beaucoup plus compliqué que le premier, nous ne traitons que celui-ci...

Démonstration du théorème 4.1. Pour $N \in \mathbb{N}$, on définit le nombre $R_k(N)$ par :

$$R_k(N) = \sum_{m=0}^{N} r_k(m)$$

Il est clair que $R_k(N)$ représente le nombre de solutions dans $\mathbb{N}^k$ de

$$x_1^n + \cdots + x_k^n \leq N. \tag{2}$$

Si on considère un k-uplet d'entier naturels, une condition suffisante (mais non nécessaire) pour qu'il soit solution de l'inégalité 2 est

$$\forall i \in [\![1, k]\!], \quad 0 \leq x_i \leq \left(\frac{N}{k}\right)^{\frac{1}{n}}.$$

Comme $x_i \in \mathbb{N}$, cette condition équivaut à $x_i \in \left[\!\!\left[1, E\left(\left(\frac{N}{k}\right)^{\frac{1}{n}}\right)\right]\!\!\right]$. Après avoir choisi les x_i dans cet intervalle, on peut les permuter, on a donc :

$$R_k(N) \geq \left(\frac{N}{k}\right)^{\frac{k}{n}}. \tag{3}$$

Supposons $\sigma(kA_n) = 0$, comme $1 \in kA_n$, on sait que pour tout $\varepsilon > 0$, il existe N tel que $(kA_n)(N) < \varepsilon N$. Dans la somme définissant $R_k(N)$, seuls les termes où $m \in kA_n > 0$ sont non-nuls, il y en a donc $(kA_n)(N)$. On applique la majoration du lemme fondamental :

$$R_k(N) = r_k(0) + \sum_{m=1}^{N} r_k(m) < 1 + CN^{\frac{k}{n}-1}(kA_n)(N) < 1 + C\varepsilon N^{\frac{k}{n}}.$$

On a utilisé le fait que $r_k(0) = 1$. Or, on peut prendre l'entier N aussi grand qu'on veut, par exemple assez grand pour que $1 < C\varepsilon N^{\frac{k}{n}}$, pour ce choix de N on a donc :

$$R_k(N) < 2C\varepsilon N^{\frac{k}{n}}.$$

On peut maintenant choisir notre ε de telle sorte que $2C\varepsilon < \left(\frac{1}{k}\right)^{\frac{k}{n}}$. Pour ce choix de ε et l'entier N adapté, on a :

$$R_k(N) < \left(\frac{N}{k}\right)^{\frac{k}{n}}.$$

C'est en contradiction avec l'inégalité 3, notre hypothèse sur la densité de kA_n est donc fausse, et $\sigma(kA_n) > 0$, ce qui conclut la preuve du théorème. □